CSBR Signing Service

CA/Browser Forum CSWG

June 2021

Plan to discuss

- Current CSBR requirements
- Discussion Items
- Some Models

Definition

- **Signing Service**: An organization that signs Code on behalf of a Subscriber using a Private Key associated with a Code Signing Certificate.

Note: Definition does not indicate who the certificate is issued to

Warranties

- **Compliance**. The CA and any Signing Service each represents that it has complied with these Requirements and the applicable Certificate Policy and Certification Practice Statement in issuing each Code Signing Certificate and operating its PKI or Signing Service.
- **Identity of Subscriber**: At the time of issuance, the CA or Signing Service represents that it (i) operated a procedure for verifying the identity of the Subscriber that at least meets the requirements in Section 11 of this document, (ii) followed the procedure when issuing or managing the Certificate, and (iii) accurately described the same procedure in the CA's Certificate Policy or Certification Practice Statement.
- **Key Protection:** The CA represents that it provided the Subscriber at the time of issuance with documentation on how to securely store and prevent the misuse of Private Keys associated with Code Signing Certificates, or in the case of a Signing Service, securely stored and prevented the misuse of Private Keys associated with Code Signing Certificates;
- **Subscriber Agreement:** The CA and Signing Service represent that the CA or Signing Service entered into a legally valid and enforceable Subscriber Agreement with the Applicant that satisfies these Requirements or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use.

Why does the Signing Service need a Subscriber agreement with the Subscriber? Isn't the Subscriber Agreement with the CA?

Model

- “Timestamp” method and the “Signing Service” methods permit Code to remain valid for longer periods of time
- Signing Service Method: In this method, the Subscriber uses the service to sign compiled code, binary, file, app, or similar object. Alternatively, the service MAY sign a digest of the preceding objects. The resulting Code Signature is valid up to the expiration time of the Signing Service’s Code Signing Certificate and any applicable revocation date, whichever comes first. Signing Services MAY also timestamp signed Code.

Note: Signing Service model DOES NOT permit code to remain valid for longer periods of time unless there is a longer certificate validity period.

Validity Period

- The validity period for a Code Signing Certificate issued to a Subscriber or Signing Service MUST NOT exceed 39 months.
- Note that the old EV document stated “Timestamp Authorities and Signing Authorities may obtain an EV Timestamp Certificate or EV Code Signing Certificate (respectively) with a validity period not exceeding one hundred and thirty five months. This is probably why the model states “for longer periods of time”.

Signing Request

- Prior to signing Code, the Signing Service MUST obtain from the Applicant a signing request in a form prescribed by the Signing Service and that complies with these Requirements. One signing request MAY suffice for multiple Code Signatures for the same Applicant, subject to the requirements specified herein. The signing request MAY be made, submitted and/or signed electronically.
- The certificate request or signing request MAY include all factual information about the Applicant necessary to issue the Certificate or sign the Code, and such additional information as is necessary for the CA or Signing Service to obtain from the Applicant in order to comply with these Requirements and the CA's Certificate Policy and/or Certification Practice Statement. In cases where the certificate request or signing request does not contain all the necessary information about the Applicant, the CA or Signing Service MUST obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. The CA or Signing Service MUST establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.
- For Certificates transported outside of a Signing Service's secure infrastructure, the CA or Signing Service MUST require, by contract, each Subscriber to generate their own Private Key and protect the Private Key in accordance with Section 16.2 ("Private Key Protection").

Delegation

- The CA MUST verify that the Signing Service and any other Delegated Third Party’s personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 14 of this document and the document retention and event logging requirements of Section 15 of this document.

Key Protection

- The Signing Service MUST ensure that a Subscriber’s private key is generated, stored, and used in a secure environment that has controls to prevent theft or misuse. A Signing Service MUST enforce multi-factor authentication to access and authorize Code Signing and obtain a representation from the Subscriber that they will securely store the tokens required for multi-factor access. A system used to host a Signing Service MUST NOT be used for web browsing. The Signing Service MUST run a regularly updated antivirus solution to scan the service for possible virus infection. The Signing Service MUST comply with the Network Security Guidelines as a “Delegated Third Party”.
- For EV Code Signing Certificates, Signing Services shall protect private keys in a FIPS 140-2 level 2 (or equivalent) crypto module. After 2021-06-01, the same protection requirements SHALL apply to Non EV Code Signing Certificates.

Audit

- Audits MUST be conducted for all obligations under these Guidelines, including timestamping and signing services , regardless of whether they are performed directly by the CA or by a Delegated Third Party. Functions performed by a Delegated Third Party MUST be included in the CA's audit or the CA MUST obtain an audit report from the Delegated Third Party. If the opinion is that the Delegated Third Party does not comply, then the CA MUST not allow the Delegated Third Party to continue performing delegated functions.

Understanding of the Signing Service Model

- The Signing Service is an RA which can validate all Applicant's information, approve an Applicant, create a key for the Subscriber, request a certificate from the CA, and sign code per Subscriber's request
- Note:
  - Signing Service could be a third party
  - Signing Service could have their own Private Key and Code Signing Certificate
  - Signing Service accepts Signing Requests from Applicants
  - Signing Service needs to verify Applicants the same as a CA
  - Signing Service must verify all data requested for inclusion in the Certificate by the Applicant
  - Signing Service must manage Private Keys on an HSM
  - Signing Service accepts signing requests
  - Signing Service must be audited

Discussion Items

- Signing Service SHALL generate and manage Subscriber keys in an HSM
    - Keys SHALL NOT be imported or exported
- Private Key activation MUST require Subscriber's authentication
- Signing Service should only be a representative of the Subscriber, NOT the CA
    - If Signing Service is to validate Subscribers, then additionally they are a Delegated Third-Party performing RA functions
- Signing Service requirements should be the same if performed by the Subscriber, a Signing Service or the CA
    - Verification must confirm keys are managed on an HSM, but NO additional audit requirements
    - In addition, WebTrust for CA section 5 is out of scope
- Code Signing certificates MUST only be issued to Subscribers, NOT to the Signing Service
- Requirements for Signing Requests and what is signed are out of scope of the CSBRs

Some Models

- Subscriber is Signing Service for its Enterprise Subscribers
- 3rd Party Signing Service generates keys for Subscribers, where the CA has validated and issued certificates to Subscribers
- 3rd Party Signing Service generates keys for Subscribers, where they are also a Delegated Third-party which ca validate Subscribers for certificates issued by the CA
- CA is Signing Service which generates keys for Subscribers, where the CA has validated and issued certificates to Subscribers

Thanks